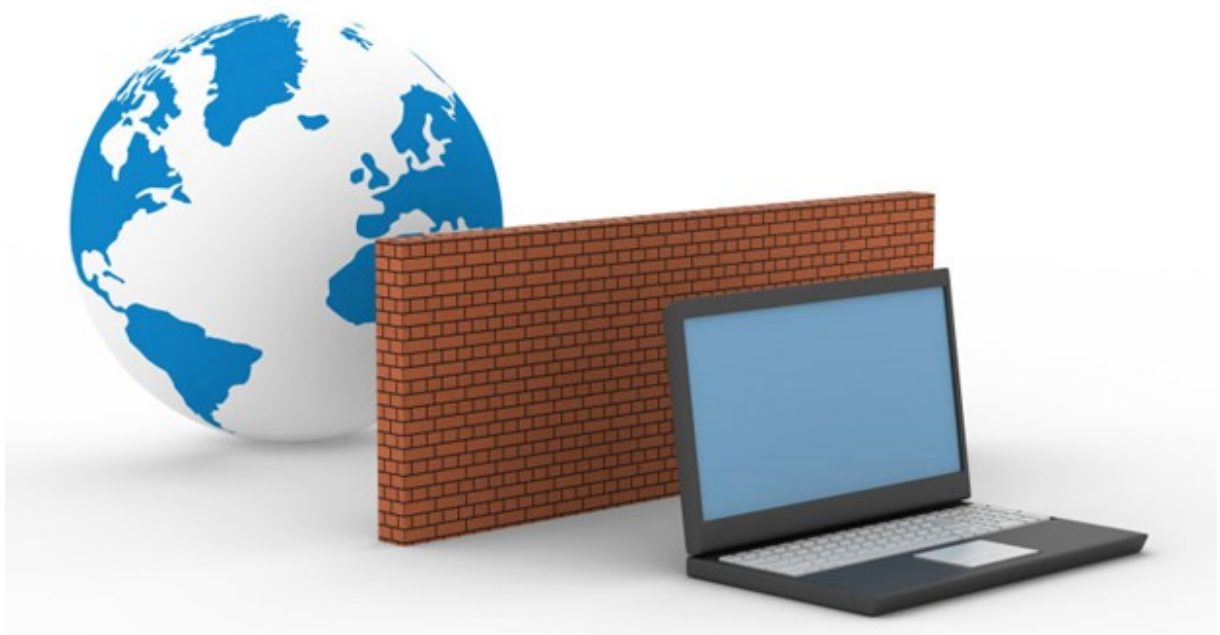


Práctica Firewall



Anais Palomera Palacios
2ºG SMR

Índice

Diagrama de red.....3

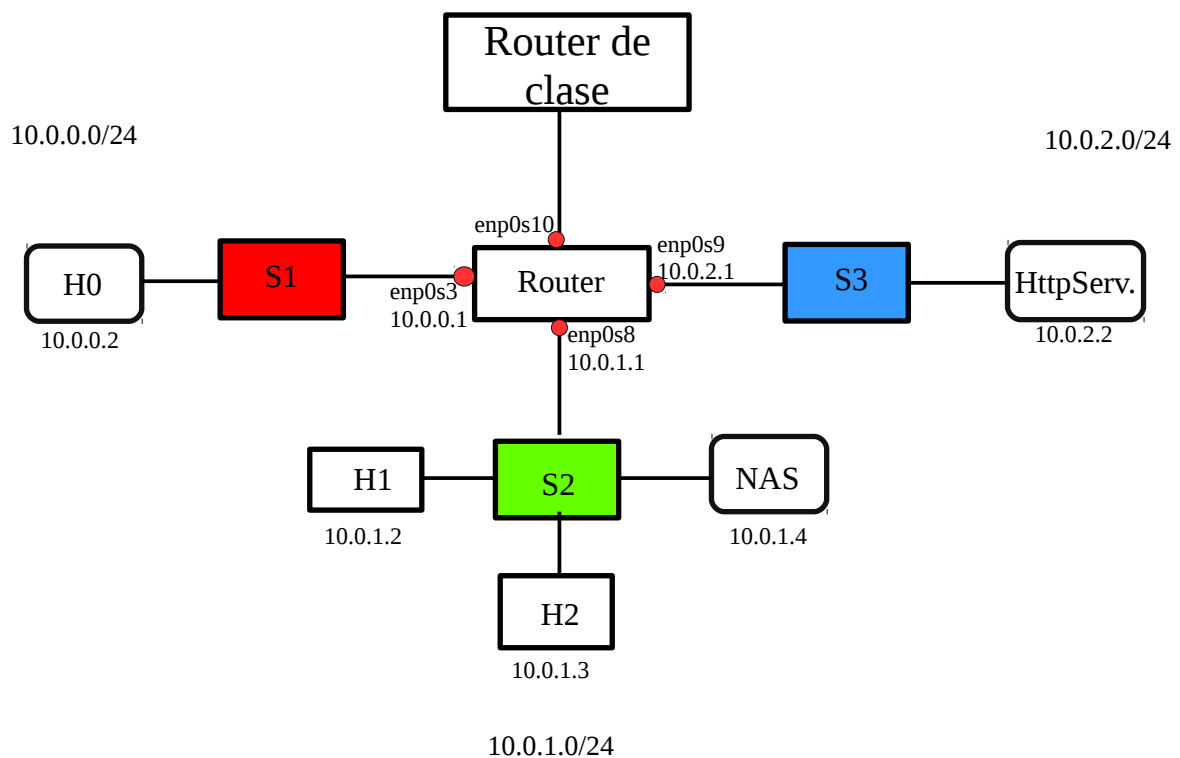
Instalar servidor http.....3

Instalar servidor NAS.....4

Script para los firewall.....6

Instalar Squid de forma transparente.....6

Diagrama de red



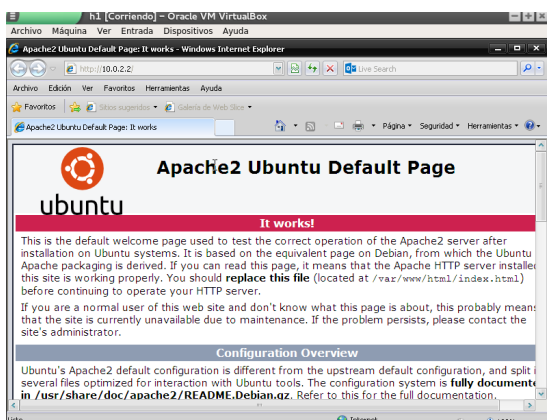
Instalar servidor http

Primero instalamos el apache2 y el vsftpd

```

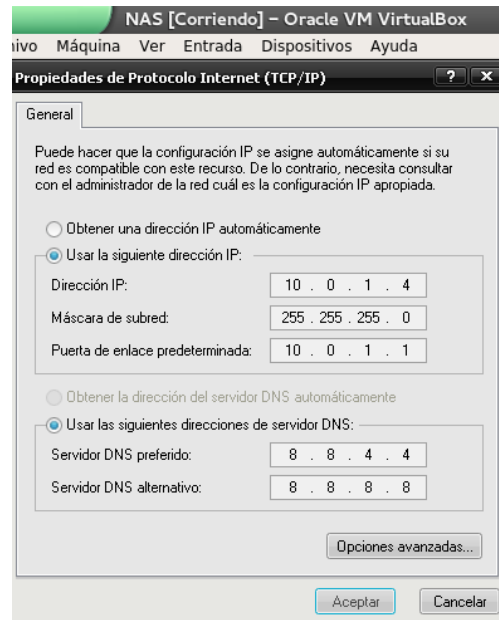
httpserv@httpserv:~$ sudo netstat -naputo
Conexiones activas de Internet (servidores y establecidos)
Proto Recib Envíad Dirección local Dirección remota Estado PID/Program name Tem
Horizador
tcp6 0 0 :::80 :::* ESCUCHAR 2254/apache2 apa
gado (0.00/0/0)
tcp6 0 0 :::21 :::* ESCUCHAR 2146/vsftpd apa
gado (0.00/0/0)
  
```

Y una vez configuradas las iptables tendremos acceso a apache y a ftp.

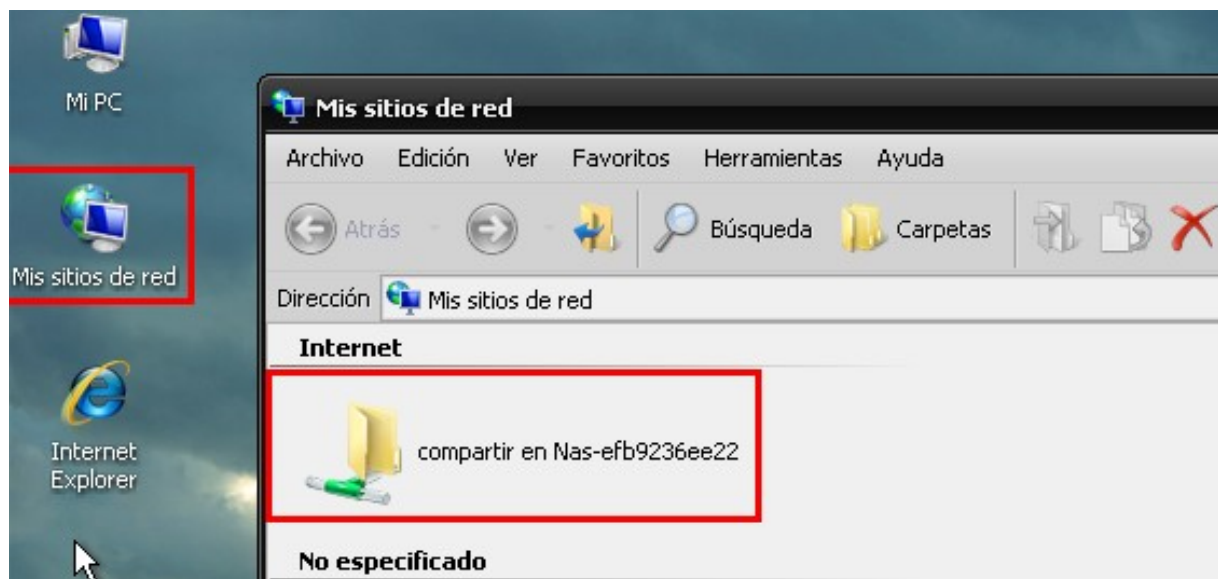


Instalar servidor NAS

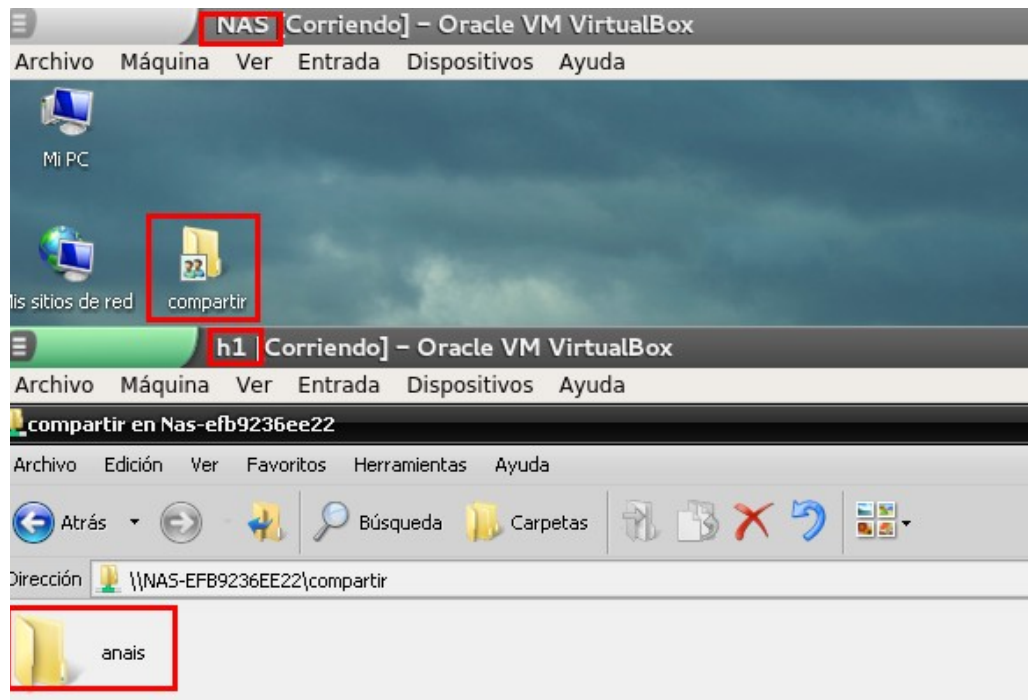
Esta es la ip del servidor NAS



Accedemos a mis sitios de red y nos aparecerá la carpeta compartida desde H1 que hemos compartido en el NAS.



Aquí se muestra la máquina **NAS** con la carpeta **compartida** y el **H1** con la carpeta **anais** que esta dentro de la compartida



Script para los firewall

```
#!/bin/bash

echo 1 > /proc/sys/net/ipv4/ip_forward

iptables -F
iptables -X
iptables -t nat -F
iptables -t nat -X
iptables -t mangle -F
iptables -t mangle -X
iptables -P INPUT DROP
iptables -P FORWARD DROP
iptables -P OUTPUT DROP

#Internet Router
iptables -t nat -A POSTROUTING -o enp0s10 -j MASQUERADE

#H0 -WIFI-- (Servidor Apache) (Internet)
iptables -A FORWARD -i enp0s3 -o enp0s10 -j ACCEPT
iptables -A FORWARD -o enp0s3 -j ACCEPT
iptables -A FORWARD -i enp0s3 -o enp0s9 -p tcp --dport 80 -j ACCEPT
iptables -A FORWARD -i enp0s3 -o enp0s9 -p udp --dport 80 -j ACCEPT

#HTTPSERV (Denegar desde H2 y NAS)
iptables -A FORWARD -s 10.0.1.3 -o enp0s9 -j REJECT
iptables -A FORWARD -s 10.0.1.4 -o enp0s9 -j REJECT

#HTTPSERV (Permitir H1)
iptables -A FORWARD -i enp0s9 -o enp0s8 -j ACCEPT
iptables -A FORWARD -i enp0s8 -o enp0s9 -j ACCEPT
iptables -A FORWARD -i enp0s8 -o enp0s9 -p tcp --dport 80 -j ACCEPT
iptables -A FORWARD -i enp0s8 -o enp0s9 -p udp --dport 80 -j ACCEPT
iptables -A FORWARD -i enp0s8 -o enp0s9 -p tcp --dport 8080 -j ACCEPT
iptables -A FORWARD -i enp0s8 -o enp0s9 -p udp --dport 8080 -j ACCEPT
iptables -A FORWARD -i enp0s8 -o enp0s9 -p tcp --dport 20 -j ACCEPT
iptables -A FORWARD -i enp0s8 -o enp0s9 -p udp --dport 20 -j ACCEPT
iptables -A FORWARD -i enp0s8 -o enp0s9 -p tcp --dport 21 -j ACCEPT
iptables -A FORWARD -i enp0s8 -o enp0s9 -p udp --dport 21 -j ACCEPT
iptables -A FORWARD -i enp0s8 -o enp0s9 -p tcp --dport 22 -j ACCEPT
iptables -A FORWARD -i enp0s8 -o enp0s9 -p udp --dport 22 -j ACCEPT

#H1
iptables -A FORWARD -m state --state RELATED,ESTABLISHED -i enp0s10 -o enp0s8 -j ACCEPT
iptables -A FORWARD -s 10.0.1.2 -o enp0s10 -j ACCEPT

#H2
iptables -A FORWARD -s 10.0.1.3 -o enp0s10 -j ACCEPT

#Squid
iptables -t nat -A PREROUTING -i enp0s3 -p tcp --dport 80 -j REDIRECT --to-port 3128
```

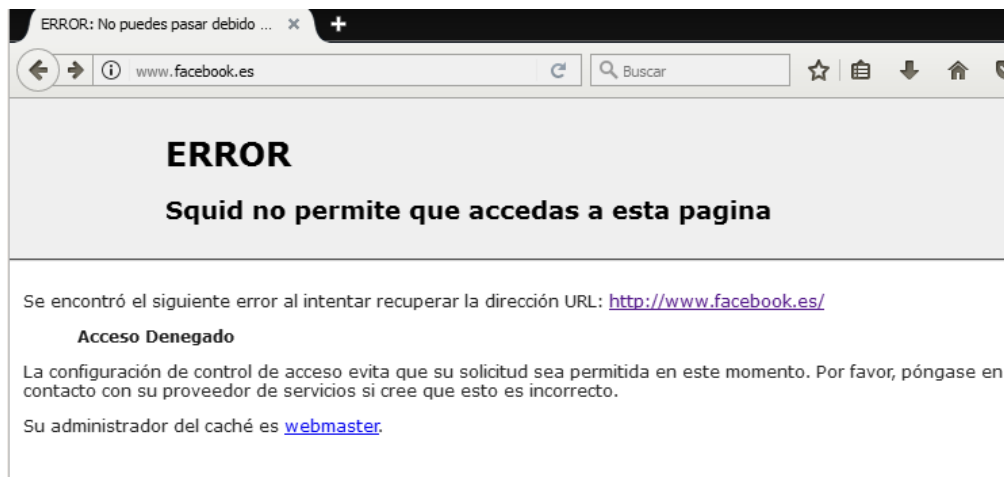
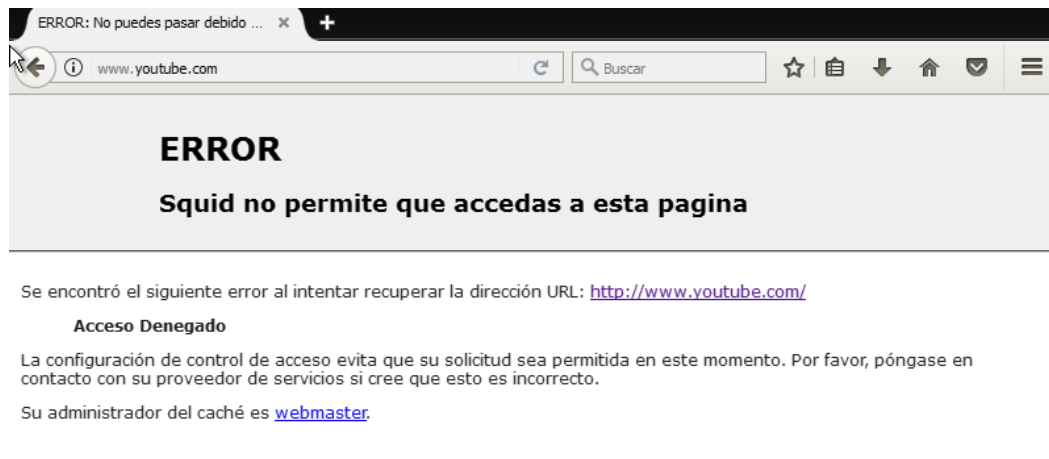
Instalar Squid de forma transparente

Squid.conf

```
acl s1 src 10.0.0.0/24
acl s2 src 10.0.1.0/24
acl s3 src 10.0.2.0/24
acl ban_domains dstdomain /etc/squid/ban_domains.txt

http_access deny ban_domains
http_access allow s1
http_access allow s2
http_access allow s3
```

```
GNU nano 2.5.3 Archivo: ban_domains.txt
www.youtube.com
www.facebook.es
```



Squid.conf

```
# Squid normally listens to port 3128
http_port 3128 transparent

# TAG: https_port
# Note: This option is only available if Squid is rebuilt with the
#       --with-openssl
```

iptables

```
#Squid  
iptables -t nat -A PREROUTING -i enp0s3 -p tcp --dport 80 -j REDIRECT --to-port 3128
```